[Company]

ACCEPTABLE USE POLICY

Acceptable use of assets

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Acceptable Use of Assets Policy

3.1 Purpose

The purpose of this policy is to make employees and external party users aware of the rules for the acceptable use of assets associated with information and information processing.

3.2 Scope

All employees and third-party users.

3.3 Principle

Use of assets is in line with applicable legislation, company policies and is in place to safeguard the company data, employees, and customers. Each user is to be responsible for their own actions and act responsibly and professionally.

3.4 Individual Responsibility

Access to the IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the company IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any company IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access company IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to company IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-company authorised device to the company network or IT systems.
- Store company data on any non-authorised company equipment.
- Give or transfer company data or software to any person or organization outside the company without the authority of the company,

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority about IT systems and data.

3.5 Internet and Email Usage

Use of the company internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the company in any way, not in breach of any term and condition of employment and does not place the individual or the company in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must **not**:

- Send or store payment card information such as:

  Payment card number (Primary Account Number or PAN)

  Security code (CVV2 etc.)

  Start and expiry dates

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which the company considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.

- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the company, alter any information about it, or express any opinion about the company unless they are specifically authorised to do this.
- Send unprotected sensitive, internal, or confidential information externally.
- Forward the company mail to personal (non-company) email accounts (for example a personal cloud or owned domain account).
- Make official commitments through the internet or email on behalf of the company unless authorised to do so.
- Download any copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download or install or distribute any software from the internet without prior approval of the IT Department.
- Connect the company devices to the internet using non-standard connections.

3.6 Working Off Site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with the company remote working policy.
- Laptop and mobile device encryption must be used.
- Laptop and mobile devices must also be protected at least by a password or a PIN.
- Equipment and media taken off-site must not be left unattended in public places including on public transport and not left in sight in a car.
- Laptops and mobile devices must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).

3.7 Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives are not to be used unless authorised. Only company owned, managed, and authorised mobile storage devices with encryption enabled must be used, when transferring internal or confidential data.

3.8 Monitoring and Filtering

All data that is created and stored on company computers is the property the company and there is no official provision for individual data privacy, however wherever possible the company will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The company has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 and any other applicable legislation.

This policy must be read in conjunction with:

• Computer Misuse Act 1990

• Data Protection Act 2018

3.9 Reporting

It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department, or the IT helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with company disciplinary procedures.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.